P/3491-US

中華民國經濟部智慧財產局

INTELLECTUAL PROPERTY OFFICE
MINISTRY OF ECONOMIC AFFAIRS
REPUBLIC OF CHINA

茲證明所附文件，係本局存檔中原申請案的副本，正確無訛，
其申請資料如下：

This is to certify that annexed is a true copy from the records of this office of the application as originally filed which is identified hereunder:

申　請　日：西元 2000 年 07 月 29 日
Application Date

申　請　案　號：089115204
Application No.

申　請　人：林海
Applicant(s)

局　　長
Director General

陳明邦

發文日期：西元2001 年 3 月14 日
Issue Date

發文字號：09011003696
Serial No.

申請日期：	案號：
類別：	

（以上各欄由本局填註）

發明專利說明書

一、發明名稱	中 文	一種防止垃圾電子郵件的方法
	英 文	Method of Anti-Spam
二、發明人	姓 名（中文）	1. 林海
	姓 名（英文）	1. Lin Hai
	國 籍	1. 中國
	住、居所	1. 中國上海市閔行區北橋村七林14號
三、申請人	姓 名（名稱）（中文）	1. 林海
	姓 名（名稱）（英文）	1. Lin Hai
	國 籍	1. 中國
	住、居所（事務所）	1. 中國上海市閔行區北橋村七林14號
	代表人姓 名（中文）	1.
	代表人姓 名（英文）	1.

四、中文發明摘要　（發明之名稱：一種防止垃圾電子郵件的方法）

一種防止垃圾電子郵件的方法，為電子郵件位址（E-MAIL ADDRESS）設立一個可選的信任碼，一個信任名單組，一個或多個基於WEB的在線發送郵件的網站（信任發信站）。初次，發送者發郵件給接收者，被強制選用如下兩種方式：一，訪問接收者的信任發信站在線發送；二，以其他方式發送，但必須在郵件中包含接收者的信任碼。以後，由於發送者已被自動存入接收者的信任名單組，再次發郵件時即可恢復一般的方式。

英文發明摘要　（發明之名稱：Method of Anti-Spam）

本案已向

國(地區)申請專利	申請日期	案號	主張優先權
無			

有關微生物已寄存於

寄存日期	寄存號碼
無	

五、發明說明 (1)

發明領域

本發明涉及電子郵件(E-MAIL)，是防止垃圾電子郵件的一種方法。

發明背景

電子郵件作為方便的通信交流方式，已被廣泛應用，成為我們工作生活的一部分。人們在享受電子郵件諸多的優點的同時，往往也為收到越來越多的垃圾電子郵件所煩惱。

目前對付垃圾電子郵件的方法是過濾技術。即接收者指定一組不受歡迎的發送者電子郵件位址(E-MAIL ADDRESS)或特定條件的字串，用於過濾掉垃圾郵件。參閱：

美國專利 6023723
加拿大專利 2282502
PCT專利 WO 98/00787
PCT專利 WO 98/37680
PCT專利 WO 99/32985
PCT專利 WO 99/37066
PCT專利 WO 99/67731

五、發明說明 (2)

發明概要

過濾技術確實能阻止部分垃圾郵件，已被廣泛應用。但其缺點也是顯而易見的：(1)接收者事先並不知道垃圾郵件發送者的電子郵件位址，並且，垃圾郵件發送者經常變換發送者的電子郵件位址，甚至更本就不留下發送者的電子郵件位址。(2)通過特定的字串(例如在郵件標題中出現某個單詞)來判斷是否垃圾郵件，在實際應用中只能起有限的效果。(3)過濾技術需要電子郵件接收者不斷付出勞動來設定過濾條件。

發明詳細說明

本發明的目的，是提供一種有效的方法，防止垃圾電子郵件。說明如下：

1)為電子郵件位址設立一個信任碼(TRUSTCODE)。信任碼為一字串。信任碼是可選項，即電子郵件接收者可決定是否選用信任碼。接收者可隨時更改其信任碼。例如：電子郵件位址username@mailserver.com信任碼tc2000。有兩種方式設立信任碼：其一，設立在接收者的電子郵件伺服器系統上；其二，設立在接收者的電子郵件用戶端系統上。

2）為電子郵件位址設立一個信任名單組(TRUSTLIST)。信任名單組存儲發送者的電子郵件位址。有兩種方式設立信任名單組：其一，設立在接收者的電子郵件伺服器系統上；其二，設立在接收者的電子郵件用戶端系統上。

3）為電子郵件位址設立一個或多個基於WEB的在線發送電子郵件的網站，稱為信任發信站(TRUSTWEB)。有兩種方式設立信任發信站：其一，在目標電子郵件位址所在的網域名稱(DOMAIN NAME)上設立發信站，作為基於該網域名稱的電子郵件位址的信任發信站，稱為私有信任發信站(PRIVATE TRUSTWEB)；其二，在其他網域名稱上設立若干個發信站，作為所有電子郵件位址的可選的信任發信站，稱為公共信任發信站(PUBLIC TRUSTWEB)。

4）當發送者的電子郵件位址還沒有被存入接收者的信任名單組時，強制發送者選用如下兩種方式發送電子郵件：

第一，訪問接收者的信任發信站，以基於WEB的方式在線發送郵件給接收者。例如，接收者的電子郵件位址為username@mailserver.com，其信任發信站為www.mailserver.com，則發送者需上網訪問該網站，使用網站上提供的基於WEB的功能在線發送郵件給接收者。

五、發明說明（4）

第二，以其他方式發送，包括用電子郵件用戶端軟體以SMTP方式發送，但必須在發出的郵件中包含接收者的信任碼資訊。

如果接收者未設立信任碼，則強制該發送者選用所說第一種方式。

5）當發送者按以上所說兩種方式發送的郵件到達接收者的電子郵件伺服器或被接收者下載之後，發送者的電子郵件位址被自動存入接收者的信任名單組。

6）當發送者的電子郵件位址已經被存入接收者的信任名單組後，發送者給接收者發電子郵件時可採用任意方式發送，不必從接收者的信任發信站在線發送，也不必在所發出的郵件中包含接收者的信任碼資訊。

7）在發出的郵件中包含接收者的信任碼資訊，有如下方式：

7-1）將信任碼資訊編碼在目標電子郵件位址中。方法之一，將信任碼作為電子郵件位址中的用戶名的尾碼，以一個分割字元"-"作為用戶名和信任碼的分界，使用戶名加上字元"-"再加上信任碼，組成一個新的用戶名，新用戶名與原網域名稱(DOMAIN NAME)一起組成一個新的電子郵

件位址。例如：

電子郵件位址為username@mailserver.com，其信任碼為tc2000，

編碼後的電子郵件位址為

username-tc2000@mailserver.com，

發送給username-tc2000@mailserver.com的電子郵件到達其伺服器後，伺服器系統自動解析出目標信箱為username@mailserver.com，信任碼為tc2000。

7-2)將信任碼資訊編碼在發出郵件的標題中。方法之一，將信任碼包含在一對分割字元"<"和">"之間，附加在郵件標題上。例如：

編碼前標題為 Subject: hello

編碼後標題為 Subject: hello <tc2000>

其中tc2000 是目標電子郵件位址的信任碼。

7-3)將信任碼資訊編碼在發出郵件的正文中。方法之一，將信任碼作為郵件正文的第一行。

7-4)在郵件格式中設立專門的一項為信任碼。目前郵件格式主要是以下幾項：

From: 發送者電子郵件位址

Reply-to: 回信用電子郵件位址

To: 接收者電子郵件位址

五、發明說明 (6)

Subject: 郵件標題

Body: 郵件正文

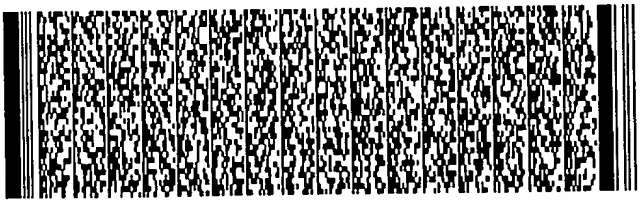
在郵件格式中設立"信任碼"，使發出的電子郵件中包含這一新項:

Trustcode: 接收者的信任碼

8)如果接收者未設立信任碼，當發送者的電子郵件位址還沒有被存入接收者的信任名單組時，發送者發電子郵件給接收者，如果採用了"訪問接收者的信任發信站在線發送"之外的方式，則郵件被退回，在退回的郵件中有預先設定的內容，提示發送者訪問接收者的信任發信站在線發送。

9)如果接收者設立了信任碼，當發送者的電子郵件位址還沒有被存入接收者的信任名單組時，發送者發電子郵件給接收者，如果採用了"訪問接收者的信任發信站在線發送"之外的方式，但沒有在發出郵件中包含接收者的信任碼，則郵件被退回，在退回的郵件中有預先設定的內容，提示發送者提供正確的信任碼或訪問接收者的信任發信站在線發送。

按以上所說方法可知，垃圾郵件發送者由於不知道海量電子郵件位址的信任碼，不能採用傳統的方式大批量發送電子郵件。而訪問每個目標電子郵件位址的信任發信站在線發送，則不適合於大批量自動操作。由此，垃圾電子



郵件被阻止。接收者可隨時改變其電子郵件位址的信任碼，以便於在老的信任碼不慎泄露之後可繼續阻止垃圾郵件，而不必改變其電子郵件位址，不影響正常的通信。

本發明阻止垃圾電子郵件的代價是，給接收者發第一封電子郵件時，發送者需在線訪問接收者的信任發信站，或需知道接收者的信任碼。這樣給發送者增加了麻煩。當再次發送郵件給同一接收者時，由於發送者的電子郵件位址已經被存入接收者的信任名單組，發送者可採用現在通行的方式，因而麻煩僅限於初次發送。當然，接收者可事先將可信任的發送者的電子郵件位址存入其信任名單組，以方便發送者。

為電子郵件位址設立信任碼的目的是，使接收者可事先將其信任碼告訴可信任的發送者，以便於發送者首次發送電子郵件給接收者時，可使用流行的用戶端軟體，而不必在線訪問接收者的信任發信站。另外，由於信任碼如7-1）所說可隱含在電子郵件位址中，與現行的電子郵件位址格式相容，可保證接收者正常使用各種基於電子郵件的服務，比如在郵件列表（MAILING LIST）登記等。郵件列表服務通常採用自動大批量發送的方式。為使用這些服務，接收者為其電子郵件位址設立信任碼是必要的。例如，接收者電子郵件位址username@mailserver.com，以此地址在某郵件列表登記，如上所說，郵件列表服務發來的郵件

將被退回，如果接收者設立了信任碼tc2000，則在郵件列表登記時可使用隱含信任碼的地址username-tc2000@mailserver.com，這樣即可正常使用郵件列表服務了。

本發明與傳統的過濾技術相比，無須事先知道誰是垃圾電子郵件發送者，無須猜測來信是否垃圾電子郵件，無須接收者永無止境地設立過濾條件，克服了過濾技術的缺陷，可更為有效地防止垃圾電子郵件。

實施本發明，有兩種主要的方案。其一，基於電子郵件伺服器系統；其二，基於電子郵件用戶端系統。現分別說明：

方案一，基於電子郵件伺服器系統(E-MAIL SERVER和WEB SERVER)。

E-MAIL SERVER和WEB SERVER使用相同的網域名稱(DOMAIN NAME)。

在E-MAIL SERVER上建立如下功能：

A)解析判別來信中是否含有接收者的信任碼。

B)判別發送者電子郵件位址是否在接收者的信任名單組中。

C）自動退信功能。

D）自動更新所說的信任名單組。

作為可選項，在E-MAIL SERVER上建立識別來信是否來源於所說的公共信任發信站的功能，識別方式有判別IP地址及數位簽名等多種成熟的技術。

在WEB SERVER上建立如下功能：

A）基於WEB的在線發信功能，作為私有信任發信站，使發送者可在線發送郵件給基於該網域名稱的所有電子郵件位址。

B）使電子郵件用戶（接收者）可設立/更改所說的信任碼。

C）使電子郵件用戶（接收者）可編輯管理所說的信任名單組。

D）使電子郵件用戶（接收者）可編輯標準的自動退信內容。

作為可選項，建立若干個公共信任發信站。使發送者在公共信任發信站在線發出的電子郵件中附有該網站的數位簽名。

圖1是方案一的流程圖。

如果發送者由目標電子郵件位址的私有信任發信站發出郵件，則判斷郵件來源的過程可省略，直接轉到存儲郵件即可。

如果發送者由公共信任發信站發出郵件，則需通過識別IP位址或數位簽名等技術判斷郵件來源。

方案二，基於電子郵件用戶端系統(E-MAIL CLIENT)。

在E-MAIL CLIENT上建立如下功能：

A)使電子郵件用戶(接收者)可設立/更改所說的信任碼。

B)使電子郵件用戶(接收者)可編輯管理所說的信任名單組。

C)使電子郵件用戶(接收者)可編輯標準的自動退信內容。

D)識別來信是否來源於所說的公共信任發信站。

E)解析判別來信中是否含有接收者的信任碼。

F)判別發送者電子郵件位址是否在接收者的信任名單組中。

G)自動退信功能。

H)自動更新所說的信任名單組。

作為必選項，建立若干個公共信任發信站。使發送者在公共信任發信站在線發出的電子郵件中附有該網站的數位簽名。

圖2是方案二的流程圖。

本方案中需判斷郵件是否來源於公共信任發信站，可採用識別IP位址或數位簽名等技術。

本方案中應優化自動退信功能。如果來信較短，可在退信中附加源信件；如果來信較長或附有大文件，則不必在退信中附加源信件，或只附加源信件中的一小部分。這樣可節約退信所需的運行時間。退信的同時，將源信件從伺服器上刪除。

本方案的缺點是不能如7-1）所說將信任碼資訊隱含在目標電子郵件位址中。例如：電子郵件位址為username@mailserver.com，其信任碼為tc2000，編碼後的電子郵件位址username-tc2000@mailserver.com在其伺服器上顯然是另一個獨立的位址或非法位址。由此，用戶將不能正常使用某些基於電子郵件的服務，主要是郵件列表（MAILING LIST）服務。當然，本發明得到廣泛應用後，郵件列表服務商在用戶登記的網頁上增加一項信任碼資訊即可解決這一缺點。本方案的優點是廣大用戶立即可選用，不必等待其電子郵件服務商實施方案一。

圖式簡單說明

圖1為顯示方案(一)的流程圖

圖2為顯示方案(二)的流程圖

六、申請專利範圍

1．一種防止垃圾電子郵件的方法，其特徵在於：

為電子郵件位址設立一個信任碼(TRUSTCODE)，信任碼為一字串，信任碼是可選項，接收者可隨時更改其電子郵件位址的信任碼；

為電子郵件位址設立一個信任名單組(TRUSTLIST)，信任名單組存儲發送者的電子郵件位址；

為電子郵件位址設立一個或多個基於WEB的在線發送電子郵件的網站，稱為信任發信站(TRUSTWEB)；

當發送者的電子郵件位址還沒有被存入接收者的信任名單組時，發送者發電子郵件給接收者，被強制選用如下兩種方式：第一，訪問接收者的信任發信站，以基於WEB的方式在線發送郵件給接收者；第二，以其他方式發送，但必須在發出的郵件中包含接收者的信任碼資訊；如果接收者未設立信任碼，則該發送者只能選用所說第一種方式；

當發送者按以上所說兩種方式發送的郵件到達接收者的電子郵件伺服器或被接收者下載之後，發送者的電子郵件位址被自動存入接收者的信任名單組；

當發送者的電子郵件位址已經被存入接收者的信任名單組後，發送者給接收者發電子郵件時可採用任意方式發送，不必從接收者的信任發信站在線發送，也不必在所發出的郵件中包含接收者的信任碼資訊。

2．如申請專利範圍第1項所述的為電子郵件位址設立信任碼的方法，其特徵在於，在接收者的電子郵件伺服器系統

六、申請專利範圍

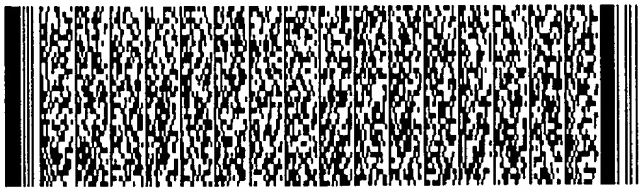
上設立其電子郵件位址的信任碼，在電子郵件到達伺服器系統時由伺服器系統判別來信中是否含有接收者的信任碼。

3．如申請專利範圍第1項所述的為電子郵件位址設立信任碼的方法，其特徵在於，在接收者的電子郵件用戶端系統上設立其電子郵件位址的信任碼，在從伺服器系統下載電子郵件時由電子郵件用戶端系統判別來信中是否含有接收者的信任碼。

4．如申請專利範圍第1項所述的為電子郵件位址設立信任名單組的方法，其特徵在於，在接收者的電子郵件伺服器系統上設立其電子郵件位址的信任名單組，當發送者按所說兩種方式發送的電子郵件到達接收者的電子郵件伺服器之後，由伺服器系統自動將發送者的電子郵件位址存入信任名單組。

5．如申請專利範圍第1項所述的為電子郵件位址設立信任名單組的方法，其特徵在於，在接收者的電子郵件用戶端系統上設立其電子郵件位址的信任名單組，發送者按所說兩種方式發送的電子郵件到達接收者的電子郵件伺服器，在被接收者下載了之後，由用戶端系統自動將發送者的電子郵件位址存入信任名單組。

6．如申請專利範圍第1項所述的一種設立信任發信站的方法，其特徵在於，在一個網域名稱(DOMAIN NAME)上設立私有的發信站，作為基於該網域名稱的電子郵件位址的信任發信站(PRIVATE TRUSTWEB)。



六、申請專利範圍

7．如申請專利範圍第1項所述的一種設立信任發信站的方法，其特徵在於，在若干個網域名稱上設立公共的發信站，作為所有電子郵件位址的可選的信任發信站(PUBLIC TRUSTWEB)。

8．如申請專利範圍第1項所述的一種防止垃圾電子郵件的方法，其特徵在於，

如果以下條件同時成立：a)接收者未設立信任碼，b)發送者的電子郵件位址還沒有被存入接收者的信任名單組，c)發送者發電子郵件給接收者，採用了"訪問接收者的信任發信站在線發送"之外的方式；那麼，將發送者發給接收者的電子郵件退回，在退信中有預先設定的內容，提示發送者訪問接收者的信任發信站在線發送；

如果以下條件同時成立：a)接收者設立了信任碼b)發送者的電子郵件位址還沒有被存入接收者的信任名單組c)發送者發電子郵件給接收者，採用了"訪問接收者的信任發信站在線發送"之外的方式，但沒有在發出郵件中包含接收者的信任碼；那麼，將發送者發給接收者的電子郵件退回，在退信中有預先設定的內容，提示發送者提供正確的信任碼或訪問接收者的信任發信站在線發送。

9．如申請專利範圍第1項所述的發送電子郵件時將接收者信任碼資訊包含在郵件中的方法，其特徵在於，

將信任碼字串編碼在目標電子郵件位址中；

將信任碼字串編碼在所發出電子郵件的標題中；

將信任碼字串編碼在所發出電子郵件的正文中；

六、申請專利範圍

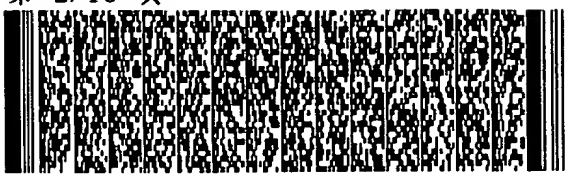
在電子郵件格式中設立專門的一項為信任碼。

10．如申請專利範圍第9項所述的將信任碼字串編碼在目標電子郵件位址中的方法，其特徵在於，將信任碼作為電子郵件位址中的用戶名的尾碼，以一個分割字元"-"作為用戶名和信任碼的分界，使用戶名加上字元"-"再加上信任碼，組成一個新的用戶名，新用戶名與原網域名稱(DOMAIN NAME)一起組成一個新的電子郵件位址。

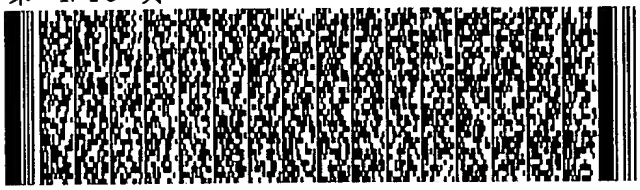
申請案件名稱：一種防止垃圾電子郵件的方法

第 1/19 頁

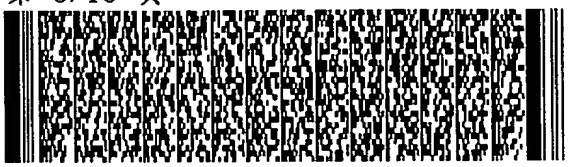
第 2/19 頁



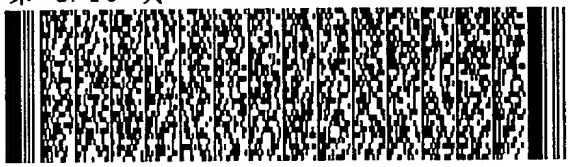
第 4/19 頁



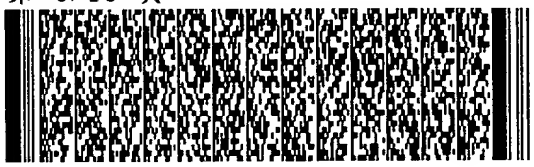
第 5/19 頁



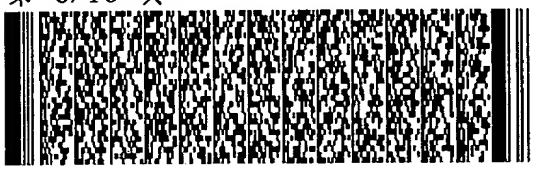
第 5/19 頁



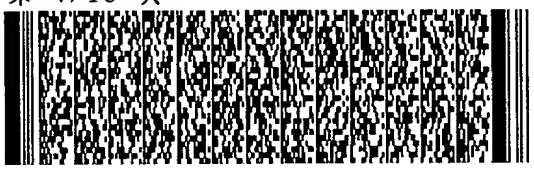
第 6/19 頁



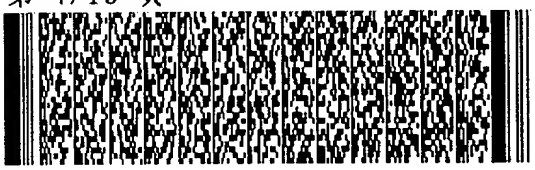
第 6/19 頁



第 7/19 頁

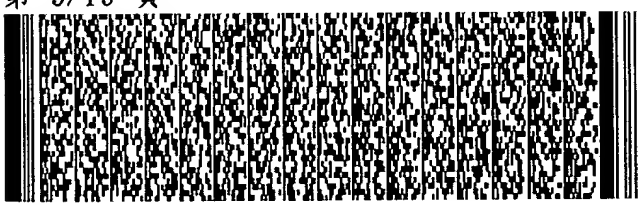


第 7/19 頁

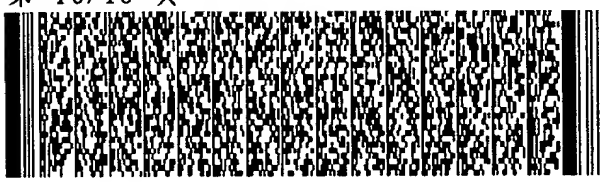


第 8/19 頁

第 9/19 頁



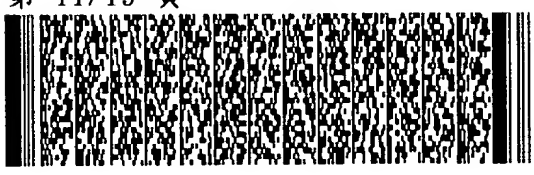
第 10/19 頁



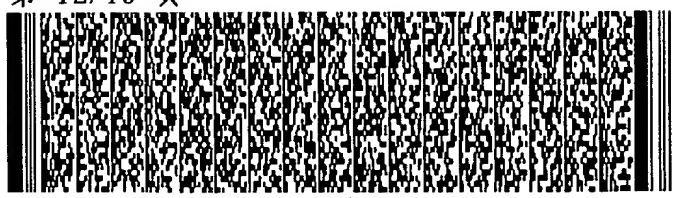
第 10/19 頁

第 11/19 頁

第 11/19 頁

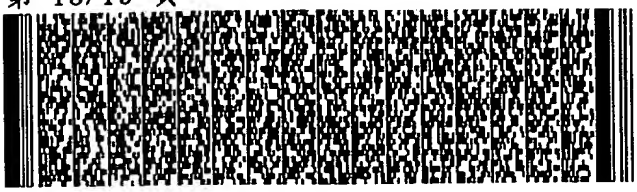


第 12/19 頁

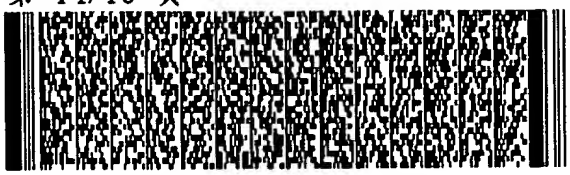


申請案件名稱：一種防止垃圾電子郵件的方法

第 13/19 頁



第 14/19 頁



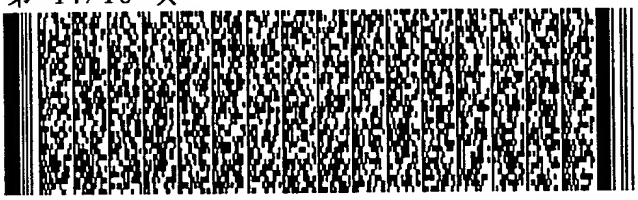
第 14/19 頁

第 15/19 頁

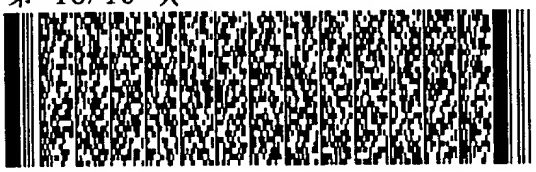
第 16/19 頁

第 16/19 頁

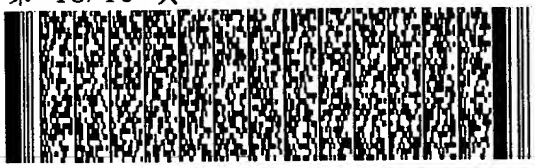
第 17/19 頁



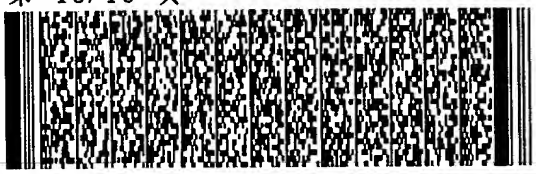
第 18/19 頁



第 18/19 頁



第 19/19 頁



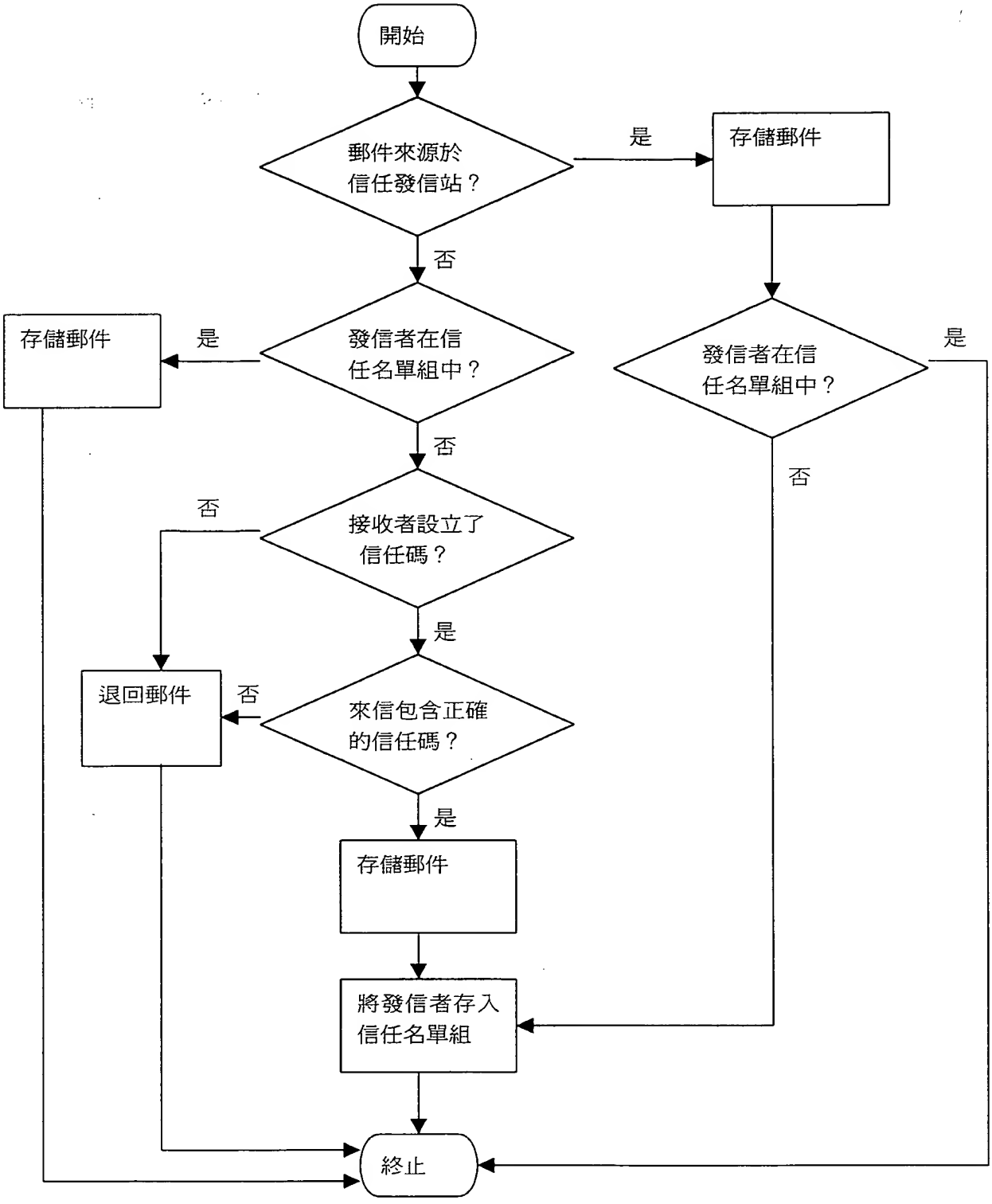

開始
郵件來源於
信任發信站？
是
存儲郵件
否
存儲郵件
是
發信者在信
任名單組中？
發信者在信
任名單組中？
是
否
否
接收者設立了
信任碼？
否
是
退回郵件
否
來信包含正確
的信任碼？
是
存儲郵件
將發信者存入
信任名單組
終止

圖 1

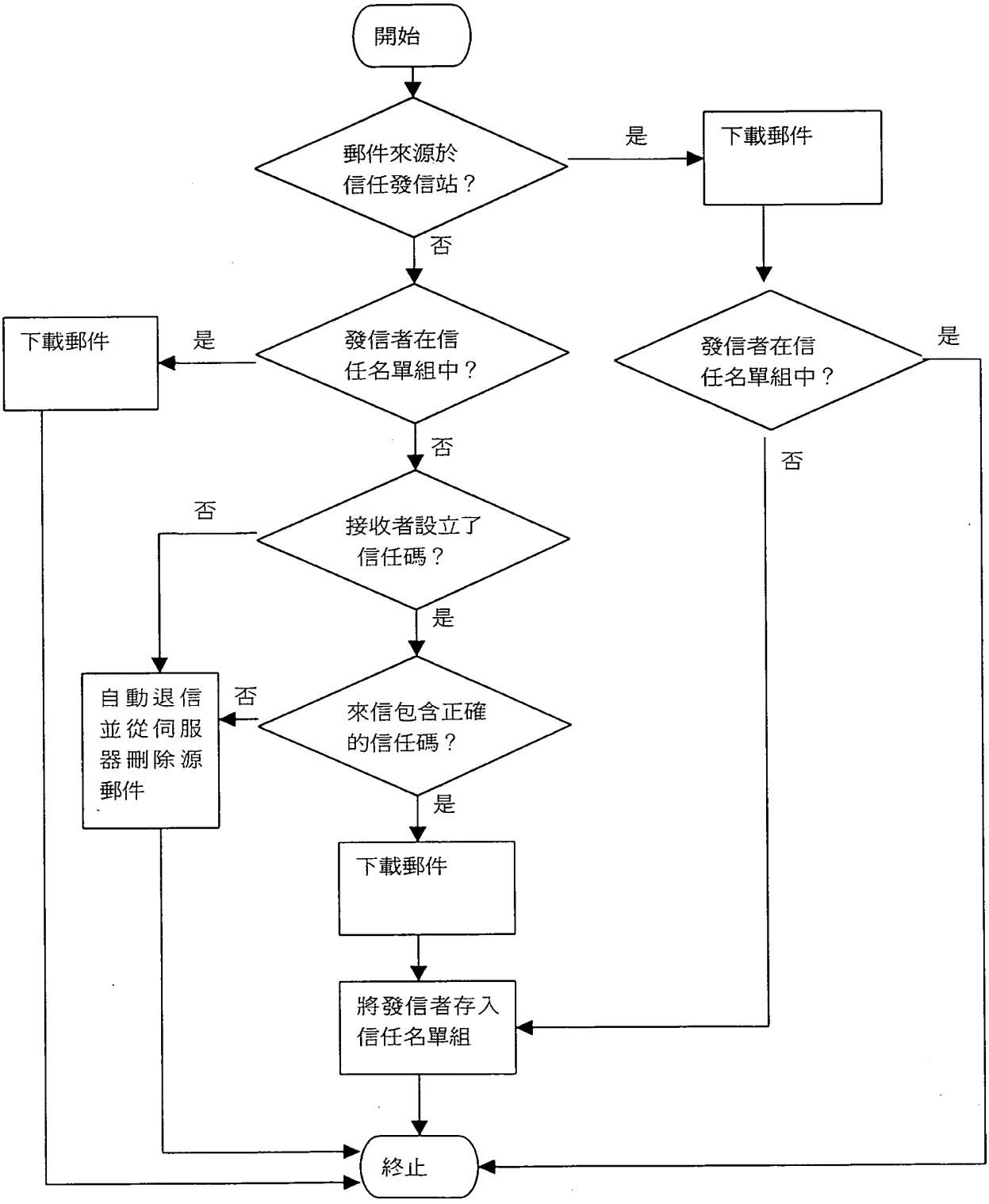

開始
郵件來源於信任發信站？
是
下載郵件
否
發信者在信任名單組中？
是
下載郵件
發信者在信任名單組中？
是
否
否
接收者設立了信任碼？
否
是
自動退信並從伺服器刪除源郵件
否
來信包含正確的信任碼？
是
下載郵件
將發信者存入信任名單組
終止

圖 2